



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/020,470	10/30/2001	Wei-Qiang Michael Gui	13768.209	9272
47973 7590 04/02/2007 WORKMAN NYDEGGER/MICROSOFT 1000 EAGLE GATE TOWER 60 EAST SOUTH TEMPLE SALT LAKE CITY, UT 84111			EXAMINER DEBNATH, SUMAN	
			ART UNIT 2135	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE			MAIL DATE	DELIVERY MODE
3 MONTHS			04/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/020,470

Applicant(s)

GUI ET AL.

Examiner

Suman Debnath

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10/30/2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-40 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-40 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 10/30/2001.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-40 are pending in this application.

Claim Objections

2. Claims 2 and 28 are objected to for minor informalities. The claims recite that the act of receiving an authentication request at "the authentication" (see claim 2, line 3; claim 28, line 3). It is assumed that the applicant intended to claim that the act of receiving an authentication request at "the authentication system."
3. Claim 12 recites that "the authentication system that is more secure **that** the access credential" in line 4. It is assumed that the applicant intended to claim "the authentication system that is more secure **than** the access credential."
4. Claim 12 is objected to because its recitation to "a specific level of security" is unclear as to what exactly the applicant is attempting to claim. How specific is "a specific level of security"?
5. Claim 22 is objected to because it recites, "a master **credentials**" in line 8. It is assumed that the applicant intended to claim "a master credential."
6. Claim 26 is objected to because its recitation to "substantially numerical input" is unclear as to what exactly applicant is attempting to claim. How substantially is "substantially numerical input"?

Appropriate correction is required.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1 and 27 are rejected under 35 U.S.C. 102(e) as being anticipated by Moreh et al. (Patent No.: US 6,959,336 B2), hereinafter "Moreh".

8. As to claim 1, Moreh discloses in a system including a service that is accessed by a user from one or more devices with varying input capabilities, a method for associating multiple credentials with a single user account such that the user may be authenticated with any one of the multiple credentials (abstract), the method comprising an authentication system performing acts of:

receiving an authentication request at the authentication system from a device, wherein credentials of the user are included in the authentication request (FIG. 1, column 5, lines 45-50 and column 6, lines 5-10);

validating the credentials provided by the user, wherein the credentials are associated with a single user identifier of the user (column 6, lines 10-20, "successful authentication");

receiving new credentials from the user, wherein the new credentials are associated with the same user identifier of the user (column 6, lines 32-40, which describes registration process of credentials); and

storing the new credentials in a credential store of the authentication system such that the authentication system can authenticate the user to the service when the user provides any one of the multiple credentials ("...enters information about the authentication mechanism 32 into the mechanism repository 28" – e.g., column 6, lines 32-40, "...a subject 20 may authenticate in any environment using any type of credential." – e.g., column 6, lines 40-50).

9. As to claim 27, it is rejected using the same rationale as for the rejection of claim 1.

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 15 and 17 are rejected under 35 U.S.C. 102(b) as being anticipated by Laursen et al. (Patent No.: US 6,065,120), hereinafter "Laursen".

12. As to claim 15, Laursen discloses in a system wherein a user is authenticated to multiple services by an authentication system, a method for authenticating the user to

Art Unit: 2135

each of the multiple services when the user accesses the multiple services with one or more devices that have different input capabilities (abstract), the method comprising acts of:

validating a credential supplied by the user, wherein the credential is associated with a user account and wherein the user account includes a user identifier that authenticates the user to each of the multiple services (FIG. 2b, column 7, lines 45-65 and column 8, lines 5-26);

associating a new credential provided by the user with the user account, wherein the new credential corresponds to the input capabilities of a device (FIG. 2b, column 7, lines 10-15, column 8, lines 4-35); and

storing the new credential in a credential store for use in authenticating the user when the user provides the new credential for authentication (FIG. 2b, item 130, column 7, lines 40-45).

13. As to claim 17, Laursen discloses a method wherein the authentication system is a distributed system, wherein the act of associating a new credential provided by the user with the user account further comprises an act of symmetrically associating the new credential with the user account such that the user account is linked with the new credential (FIG. 2b, column 8, lines 4-35).

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

15. Claims 4-6, 9-11, 30-32 and 35-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh in view of Laursen.

16. As to claims 4 and 30, Moreh doesn't explicitly disclose the act of receiving new credentials from the user further comprises an act of symmetrically associating the new credentials with a user identifier. However, Laursen discloses the act of receiving new credentials from the user further comprises an act of symmetrically associating the new credentials with a user identifier (column 8, lines 4-35).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh by symmetrically associating the new credentials with a user identifier as taught by Laursen in order to "perform transactions or retrieve pertinent information without the need to key in such every time the transactions or the information are desired." (Laursen)

17. As to claims 5 and 31, Moreh doesn't explicitly disclose the act of symmetrically associating the new credential with a user identifier further comprises an act of associating the new credentials with a user account. However, Laursen discloses the

act of symmetrically associating the new credential with a user identifier further comprises an act of associating the new credentials with a user account (column 8, lines 4-35).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh by associating the new credentials with a user account as taught by Laursen in order to "perform transactions or retrieve pertinent information without the need to key in such every time the transactions or the information are desired." (Laursen)

18. As to claims 6 and 32, Moreh doesn't explicitly disclose the act of symmetrically associating the new credential with a user identifier further comprises an act of caching a copy of the user identifier with the new credential. However, Laursen discloses an act of caching a copy of the user identifier with the new credential (FIG. 2b, column 8, lines 4-35).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh by including an act of caching a copy of the user identifier with the new credential as taught by Laursen in order to "perform transactions or retrieve pertinent information without the need to key in such every time the transactions or the information are desired." (Laursen)

19. As to claim 9, Moreh discloses in a system that includes multiple services that are accessed by a user over a network such as the Internet, wherein the user accesses

Art Unit: 2135

the multiple services from one or more devices that have varying input capabilities, a method for accessing a service from a device (abstract), the method comprising acts of:

providing multiple credentials to an authentication service, wherein each of the multiple credentials that is maintained by the authentication system (FIG. 1, column 6, lines 40-56);

requesting access to a service using a device included in the one or more devices, wherein the service requires that the user be authenticated before access to the service is granted to the user, wherein the device is redirected to the authentication system (column 5, lines 38-56 and column 6, lines 7-20);

selecting an access credential to send to the authentication system from the multiple credentials and entering the access credential in the device (column 6, lines 62-67 to column 7, lines 1-4);

issuing an authentication request to an authentication system, wherein the authentication request includes the access credential selected by the user (column 7, lines 15-28, column 9, lines 49-52);

receiving an authentication response from the authentication system, wherein the authentication response includes a user identifier that authenticates the user to the service if the access credential is validated (“...authentication response which it transmits back to the client 22” – e.g. column 6, lines 13-20); and

sending an authenticated request to the service, wherein the authenticated request includes the user identifier such that access to the service is obtained (“...the

client 22 delivers the authentication response to the server application 38.” – e.g. see column 6, lines 20-25).

Moreh doesn't explicitly disclose that each of the multiple credentials is associated with a user account. However, Laursen discloses that each of the multiple credentials is associated with a user account (column 8, lines 4-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh by associating multiple credentials with a user account as taught by Laursen in order to “perform transactions or retrieve pertinent information without the need to key in such every time the transactions or the information are desired.” (Laursen)

20. As to claim 35, it is rejected using the same rationale as for the rejection of claim 9.

21. As to claims 10 and 36, Moreh discloses the act of selecting an access credential to send to an authentication system from multiple credentials further comprises an act of selecting the access credential according to an input capability of the device (column 6, lines 62-67 to column 7, lines 1-4).

22. As to claims 11 and 37, Moreh disclose the access credential is a numerical credential when the device has numerical input (column 6, lines 62-67 to column 7, lines 1-4).

23. Claims 7 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh in view of Leah et al. (Patent No.: US 6,986,039 B1), hereinafter "Leah".

24. As to claims 7 and 33, Moreh doesn't explicitly disclose the act of receiving new credentials from the user further comprises an act of asymmetrically associating the new credentials with a primary credential, wherein the primary credential is stored in a primary store with the user identifier. However, Leah discloses the act of receiving new credentials from the user further comprises an act of asymmetrically associating the new credentials with a primary credential, wherein the primary credential is stored in a primary store with the user identifier (FIG. 3, column 10, 48-67 – column 11, lines 1-10, which describes validating credentials with master credentials).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh by comprising an act of asymmetrically associating the new credentials with a primary credential, wherein the primary credential is stored in a primary store with the user identifier as taught by Leah in order to "synchronize credentials securely and propagate among multiple directories, operating system platforms and registries" (Leah).

25. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh in view of Leah and further in view of Wood et al. (Patent No.: US 6,609,198 B1), hereinafter "Leah".

26. As to claim 8, Moreh discloses a method further comprising one or more of:
a step for remembering which credential was received in the authentication request (column 6, lines 5-40);

Neither Moreh nor Leah explicitly disclose a step for prompting the user for a more secure credential when the credentials received in the authentication request do not meet security requirements of the service; and a step for providing at least one security measure for each credential associated with the user account, wherein the user is not authenticated to a service if the security measure of a particular credential is breached or the user account is locked.

However, Wood discloses a step for prompting the user for a more secure credential when the credentials received in the authentication request do not meet security requirements of the service (column 10, lines 25-65); and a step for providing at least one security measure for each credential associated with the user account, wherein the user is not authenticated to a service if the security measure of a particular credential is breached or the user account is locked (column 10, lines 30-35).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh and Leah as taught by Wood in order to provide "credentials without loss of session continuity" (Wood).

27. Claims 2-3, 28-29 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh in view of Wood.

28. As to claims 2 and 28, Moreh discloses wherein the act of receiving an authentication request at the authentication further comprises an act of determining where to send the credentials for validation (column 6, lines 10-20). Moreh doesn't explicitly disclose that the authentication system is a distributed authentication system. However, Wood discloses that the authentication system is a distributed authentication system (column 17, lines 15-25).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh by disclosing a distributed authentication system as taught by Wood in order to provide enhanced security to the credential repository with location transparency.

29. As to claims 3 and 29, Moreh discloses the act of determining where to send the credentials for validation uses a username of the credentials (column 6, lines 5-55).

30. As to claim 34, it is rejected using the same rationale as for the rejection of claim 8.

31. Claims 16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laursen in view of Leah.

32. As to claim 16, Laursen doesn't explicitly disclose a method wherein the act of validating a credential supplied by the user further comprises an act of locating a credential store where a master credential for the supplied credential is stored such that the supplied credential can be validated. However, Leah discloses a method wherein the act of validating a credential supplied by the user further comprises an act of locating a credential store where a master credential for the supplied credential is stored such that the supplied credential can be validated (FIG. 3, column 10, 48-67 – column 11, lines 1-10, which describes validating credentials with master credentials).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Laursen as taught by Leah in order to "synchronize credentials securely and propagate among multiple directories, operating system platforms and registries" (Leah).

33. As to claim 18, Laursen discloses a method wherein the user account is cached with the new credential (FIG. 2b, column 8, lines 4-35). Laursen doesn't explicitly disclose a method wherein the user account and the new credential are not on the same store. However, Leah discloses a method wherein the user account and the new credential are not on the same store (FIG. 3, column 10, 48-67 – column 11, lines 1-10). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Laursen as taught by Leah in order to "synchronize credentials securely and propagate among multiple directories, operating system platforms and registries" (Leah).

Art Unit: 2135

34. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Laursen in view of Wood.

35. As to claim 21, Laursen doesn't explicitly disclose a method further comprising an act of the authentication system remembering which credential is supplied by the user such that a more secure credential may be supplied by the user if a service requires more security than is provided by the supplied credential.

However, Wood discloses a method further comprising an act of the authentication system remembering which credential is supplied by the user such that a more secure credential may be supplied by the user if a service requires more security than is provided by the supplied credential (column 10, lines 25-65).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Laursen as taught by Wood in order to provide "credentials without loss of session continuity" (Wood).

36. Claims 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laursen in view of Leah and further in view of Wood.

37. As to claim 19, Laursen doesn't explicitly disclose a method wherein the authentication system is a distributed system, wherein the act of associating a new credential provided by the user with the user account further comprises an act of

Art Unit: 2135

asymmetrically associating the new credential with the user account through a primary credential, wherein the new credential is linked to the primary credential.

However, Leah discloses a method wherein the act of associating a new credential provided by the user with the user account further comprises an act of asymmetrically associating the new credential with the user account through a primary credential, wherein the new credential is linked to the primary credential (FIG. 3, column 10, 48-67 – column 11, lines 1-10, which describes validating credentials with master credentials).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Laursen as taught by Leah in order to “synchronize credentials securely and propagate among multiple directories, operating system platforms and registries.” (Leah)

Neither Laursen nor Leah explicitly discloses the authentication system is a distributed system. However, Wood teaches the authentication system is a distributed system (column 17, lines 15-25).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Laursen and Leah as taught by Wood in order to provide enhanced security to the credential repository with location transparency.

38. As to claim 20, Laursen doesn't explicitly disclose a method wherein the primary credential is cached with the new credential and wherein the primary credential and the

Art Unit: 2135

new credential are not on the same store. However, Leah discloses a method wherein the primary credential is cached with the new credential and wherein the primary credential and the new credential are not on the same store (FIG. 3, column 10, 48-67 – column 11, lines 1-10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Laursen as taught by Leah in order to “synchronize credentials securely and propagate among multiple directories, operating system platforms and registries” (Leah).

39. Claims 12-13 and 38-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh in view of Laursen and further in view of Wood.

40. As to claims 12 and 38, Neither Moreh nor Laursen explicitly disclose the service requires a specific level of security, the method further comprising: an act of requiring the user to provide a secure credential to the authentication system that is more secure than the access credential; and an act of providing the service with a level of security of the secure credential and of the access credential, wherein the service is unaware of both the selected credential and the secure credential.

However Wood discloses the service requires a specific level of security (abstract), the method further comprising:

an act of requiring the user to provide a secure credential to the authentication system that is more secure than the access credential (column 10, lines 25-65); and

an act of providing the service with a level of security of the secure credential and of the access credential, wherein the service is unaware of both the selected credential and the secure credential (column 10, lines 25-65).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh and Laursen as taught by Wood in order to provide "credentials without loss of session continuity" (Wood)

41. As to claim 13, Moreh doesn't explicitly disclose a method wherein the authentication system is a distributed system and wherein some of the multiple credentials are stored on different stores, wherein the act of providing multiple credentials to an authentication service further comprises one or more of: a step for symmetrically associating the multiple credentials with a user identifier, wherein the user identifier is cached with each of the multiple credentials; a step for symmetrically associating the multiple credentials with a user account, wherein a user account is cached with each of the multiple credentials and an step for associating a security measure with each of the multiple credentials, wherein the user is not authenticated to a service if the security measure of a particular credential is breached or the user account is locked.

However, Laursen disclose a method wherein some of the multiple credentials are stored on different stores, wherein the act of providing multiple credentials to an authentication service (abstract) further comprises one or more of:

a step for symmetrically associating the multiple credentials with a user identifier, wherein the user identifier is cached with each of the multiple credentials (column 8, lines 4-35);

a step for symmetrically associating the multiple credentials with a user account, wherein a user account is cached with each of the multiple credentials (column 8, lines 4-35) .

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh as taught by Laursen in order to “perform transactions or retrieve pertinent information without the need to key in such every time the transactions or the information are desired.” (Laursen)

Neither Moreh nor Laursen explicitly disclose a method wherein the authentication system is a distributed system and a step for associating a security measure with each of the multiple credentials, wherein the user is not authenticated to a service if the security measure of a particular credential is breached or the user account is locked. However, Wood discloses a method wherein the authentication system is a distributed system (column 17, lines 15-25) and a step for associating a security measure with each of the multiple credentials, wherein the user is not authenticated to a service if the security measure of a particular credential is breached or the user account is locked (column 10, lines 30-35).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh and Laursen as taught by Wood in order to provide “credentials without losing of session continuity” (Wood).

Furthermore, one would be motivated to do so to provide enhanced security to the credential repository with location transparency.

42. As to claim 39, it is rejected using the same rationale as for the rejection of claim 13.

43. Claims 14 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh in view of Laursen and further in view of Leah.

44. As to claims 14 and 40, neither Moreh nor Laursen explicitly disclose the authentication system is a distributed system and wherein some of the multiple credentials are stored on different credential stores, wherein the act of providing multiple credentials to an authentication service further comprises an act of asymmetrically associating the multiple credentials with a primary credential, wherein the user identifier is stored with the primary credential.

However, Leah discloses the authentication system is a distributed system and wherein the act of providing multiple credentials to an authentication service further comprises an act of asymmetrically associating the multiple credentials with a primary credential, wherein the user identifier is stored with the primary credential (FIG. 3, column 10, 48-67 – column 11, lines 1-10, which describes validating credentials with master credentials).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh and Laursen as taught by Leah in order to "synchronize credentials securely and propagate among multiple directories, operating system platforms and registries" (Leah).

45. Claims 22-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh in view of Wood, in view of Laursen and further in view of Leah.

46. As to claim 22, Moreh disclose in an environment including a user that accesses multiple services with one or more devices that have varying input capabilities, a method for an authentication system to authenticate the user to each of the multiple services (abstract), the method comprising the authentication system performing steps for:

receiving an access credential from the user (column 6, lines 62-67 to column 7, lines 1-4), and wherein the access credential has a security level (column 7, lines 29-45, "an authentication strength");

determining, from the access credential, a credential store that is used to validate the access credential (column 6, lines 10-20 and lines 32-40);

validating the access credential at the credential store (column 6, lines 10-20);

the user can be authenticated with both the access credential and the one or more new credentials, wherein each of the one or more new credentials has a security level ("...enters information about the authentication mechanism 32 into the mechanism

Art Unit: 2135

repository 28" – e.g., column 6, lines 32-40, "...a subject 20 may authenticate in any environment using any type of credential." – e.g., column 6, lines 40-50 and see also column 7, lines 29-45);

remembering the access credential that was provided by the user (column 6, lines 5-40); and

Moreh doesn't explicitly disclose that the credential is associated with a user account that includes a user identifier; a credential store that stores a master credentials and associating one or more new credentials with the user account; prompting the user for a secure credential that is more secure than the access credential if the security level of the access credential is insufficient for a service being accessed by the user, wherein the service is provided with the security level of both the access credential and the secure credential, but is not aware of either the access credential or the secure credential.

Wood discloses prompting the user for a secure credential that is more secure than the access credential if the security level of the access credential is insufficient for a service being accessed by the user, wherein the service is provided with the security level of both the access credential and the secure credential, but is not aware of either the access credential or the secure credential (column 10, lines 25-65).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh as taught by Wood in order to provide "credentials without loss of session continuity" (Wood)

Neither Moreh nor Wood explicitly disclose that the credential is associated with a user account that includes a user identifier; a credential store that stores a master credentials and associating one or more new credentials with the user account; However, Laursen discloses that the credential is associated with a user account that includes a user identifier and associates one or more new credentials with the user account (column 8, lines 4-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh and Wood by associating credentials with a user account as taught by Laursen in order to "perform transactions or retrieve pertinent information without the need to key in such every time the transactions or the information are desired." (Laursen)

Neither Moreh and Wood nor Laursen explicitly disclose a credential store that stores a master credentials. However, Leah discloses a credential store that stores a master credentials (FIG. 3).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh, Wood and Laursen by including a credential store that stores a master credentials as taught by Leah in order to "synchronize credentials securely and propagate among multiple directories, operating system platforms and registries." (Leah)

47. As to claim 23, neither Moreh nor Wood explicitly disclose a method wherein the step for associating one or more new credentials with the user account further

Art Unit: 2135

comprises a step for symmetrically associating the access credential and the one or more new credentials with the user account, wherein the user account is cached with each of the access credential and the one or more new credentials.

However, Laursen discloses a method wherein the step for associating one or more new credentials with the user account further comprises a step for symmetrically associating the access credential and the one or more new credentials with the user account, wherein the user account is cached with each of the access credential and the one or more new credentials (column 8, lines 4-35).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh and Wood by including a step for symmetrically associating the access credential and the one or more new credentials with the user account, wherein the user account is cached with each of the access credential and the one or more new credentials as taught by Laursen in order to "perform transactions or retrieve pertinent information without the need to key in such every time the transactions or the information are desired." (Laursen)

48. As to claim 24, neither Moreh, Wood nor Laursen explicitly disclose a method wherein the step for associating one or more new credentials with the user account further comprises a step for asymmetrically associating the one or more new credentials with a primary credential, wherein the primary credential is associated with the user account and wherein the primary credential is cached with each of the one or more new credentials.

However Leah discloses a method wherein the step for associating one or more new credentials with the user account further comprises a step for asymmetrically associating the one or more new credentials with a primary credential, wherein the primary credential is associated with the user account and wherein the primary credential is cached with each of the one or more new credentials (FIG. 3, column 10, 48-67 – column 11, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh, Wood and Laursen as taught by Leah in order to “synchronize credentials securely and propagate among multiple directories, operating system platforms and registries.” (Leah)

49. As to claim 25, Moreh discloses a method further comprising a step for automatically authenticating the user at different services after the user has been authenticated at a first service (column 15, lines 10-30, “....federated authentication sources that ultimately leads to global single sign-on”).

50. As to claim 26, Moreh discloses a method wherein the access credential is a numerical credential when the device has substantially numerical input (column 6, lines 62-67 to column 7, lines 1-4).

Conclusion

51. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See accompanying PTO 892.

Liao et al. (Patent Number: US 6,606,663 B1) discloses method and apparatus for caching credentials in proxy servers for wireless user agents.

Benantar (Pub. No.: US 2002/0144119 A1) discloses a system for network single sign-on.

Camacho et al. (Pub. No.: US 2003/0208684 A1) discloses a distributed personal digital identification system.

Bari et al. (Pub. No.: US 2002/0023059 A1) discloses a method for secure storage and management of personal authentication credentials data over a network.

Vandergeest et al. (Patent No.: US 6,732,277 B1) discloses a method and apparatus for dynamically accessing security credentials and related information.

Brozowski et al. (Patent No. US 6,769,068 B1) discloses dynamic credential refresh in a distributed system.

Johnson et al. (Patent Number: 5,560,008) discloses remote authentication and authorization in a distributed data processing system.

Harrison et al. (Patent No.: US 6,941,476 B2) discloses a distributed storage system for storing credentials.

Cohen et al. (Patent No.: US 6,178,511 B1) discloses coordinating user target logons in a single sign-on environment.

Kausik et al. (Pub. No.: US 2001/0034837 A1) discloses method and apparatus for secure distribution of authentication credentials to roaming users.

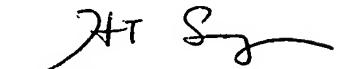
Blakley, III et al. (Patent Number: 5,604,490) discloses a method and system for providing a user access to multiple secured subsystems.

52. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SD
4D


HOSUK SONG
PRIMARY EXAMINER